Sentriant® AG Software Quick-Start Card, Version 5.4

Central Management

Extreme Networks® Sentriant® AG software includes enforcement clusters (ECs) and enforcement servers (ESs). An enforcement cluster is a logical grouping of one or more enforcement servers that are managed by a single Management server (MS).

The quarantine method is defined per cluster; all of the Enforcement servers in a given cluster use the same quarantine method (Inline, DHCP, or 802.1x). When using multiple clusters, each cluster can have a different quarantine method. Clusters cooperate to test and control access to the network.

Physical Deployment

Sentriant AG installs in one of the following ways:

- **Inline**—When deploying Sentriant AG inline, Sentriant AG monitors and enforces all device traffic. When Sentriant AG is deployed as a single-server installation, Sentriant AG becomes a Layer 2 bridge that requires no changes to the network configuration settings. When Sentriant AG is installed in a multiple-server installation, you might have to configure the switch that connects the Sentriant AG enforcement servers to use Spanning Tree Protocol (STP) if STP is not already configured.

  Sentriant AG allows devices to access the network or blocks devices from accessing the network based on their Internet Protocol (IP) address with a built-in firewall (iptables).
- **DHCP**—When deploying Sentriant AG inline with a Dynamic Host Configuration Protocol (DHCP) server, all DHCP requests pass through the Sentriant AG server(s) Layer 2 bridge. For a quarantined device, Sentriant AG distributes the quarantined IP address for the device. If Sentriant AG allows the device to have access, Sentriant AG allows your real DHCP server to distribute a non-quarantined IP address. Sentriant AG assigns a DHCP IP address based on the quarantine area parameters you define during configuration. You can place restrictions on network access either at the gateway for the device using Access Control Lists (ACLs), or on the device by removing the devices gateway and adding static routes for accessible networks.

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: April 2010
Part Number: 120574-00 Rev 01

- **802.1x**—When deploying Sentriant AG in an 802.1x environment, you must install it where it can communicate with the Remote Authentication Dial-In User Service (RADIUS) server (or, Sentriant AG has a built-in RADIUS server that you can use). The RADIUS server communicates with the switch, which performs the quarantining by moving ports or MAC addresses in and out of virtual local area networks (VLANs).

NOTE

For illustrations of these configurations, see the Installation guide, "Physical Deployment."

Ethernet Information

The Ethernet interfaces should be attached as follows:

- **eth0**—Connect to the corporate LAN (the internal network side)
- **eth1**—Connect to a switch, VPN, or DHCP server (the Internet or endpoint side)

Port Information

You might need to configure some firewalls and routers to allow Sentriant AG to access the following ports for testing:

- **Agentless test method**—137, 138, 139, and 445
- **ActiveX and agent-based test method**—4407
- **License validation and test updates**—http://update.sentriantag.extremenetworks.com
- **Software and operating system updates**—http://download.sentriantag.extremenetworks.com

Software Installation

Software installation is easy—insert the install CD-ROM, reboot the server, and follow the instructions detailed in the *Installation Guide*.

WARNING!

The install process reformats the hard drive, erasing all existing data

The install CD contains the following:

- Install image
- `/docs` directory (*Quick-start Card*, *Installation Guide*, *Users' Guide*, *Release Notes*)

NOTE

License key – *The license key is required to enable Sentriant AG operation. Your license key is emailed to you.*

User Documents

The *Installation Guide* contains the following:

- System requirements
- Install steps
- Installation and configuration check list

The *Users' Guide* contains the following:

- Configuring Sentriant AG
- Monitoring activities
- Creating NAC policies
- Running reports

The documents can be found as follows:

- In the `/docs` directory on the install CD
- By clicking the help icon from the Sentriant AG console

Customer Support

NOTE

Services can be purchased from Extreme Networks or through one of its channel partners. If you are an end-user who has purchased service through an Extreme Networks channel partner, please contact your partner first for support.

Extreme Networks Technical Assistance Centers (TAC) provide 24x7x365 worldwide coverage. These centers are the focal point of contact for post-sales technical and network-related questions or issues. TAC will create a Service Request (SR) number and manage all aspects of the SR until it is resolved. For a complete guide to customer support, see the *Technical Assistance Center User Guide* at: http://www.extremenetworks.com/go/TACUserGuide

The Extreme Networks eSupport website provides the latest information on Extreme Networks products, including the latest Release Notes, troubleshooting, downloadable updates or patches as appropriate, and other useful information and resources. Directions for contacting the Extreme Networks Technical Assistance Centers are also available from the eSupport website at: https://esupport.extremenetworks.com

Registration

If you have not already registered this product with Extreme Networks, you can register on the Extreme Networks website at: http://www.extremenetworks.com/go/productregistration

Documentation

Check for the latest versions of documentation on the Extreme Networks documentation website at:
http://www.extremenetworks.com/go/documentation

AccessAdapt, Alpine, Altitude, BlackDiamond, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is a registered trademark of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2010 Extreme Networks, Inc. All Rights Reserved.